U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

TOP TEN MANAGEMENT CHALLENGES
September 2002

MAJOR CHALLENGES FOR THE DEPARTMENT

This section highlights OIG's Top 10 Management Challenges that faced the Department at the close of this semiannual period. We view these issues as Commerce's top challenges because they meet one or more of the following criteria: they are important to the Department's mission or the nation's well-being; they are complex; they involve sizable expenditures; or they require significant management improvements. Given the diverse nature of Commerce activities, many of these issues cut across bureau and program lines. We believe that by addressing these challenges the Department can enhance program efficiency and effectiveness; eliminate serious operational problems; decrease fraud, waste, and abuse; and achieve substantial savings.

TOP 10 MANAGEMENT CHALLENGES

1. Strengthen financial management controls and systems.
2. Strengthen Department-wide information security.
3. Enhance export controls for dual-use commodities.
4. Effectively manage departmental and bureau acquisition processes.
5. Enhance emergency preparedness, safety, and security of Commerce facilities and personnel.
6. Successfully operate the U.S. Patent and Trademark Office as a performance-based organization.
7. Increase international compliance with trade agreements and expand market access for American exporters.
8. Increase the effectiveness of marine resource management.
9. Continue to improve the Department's strategic planning and performance measurement in accordance with the Government Performance and Results Act.
10. Effectively manage major Commerce renovation and construction projects.

CHALLENGE 1: STRENGTHEN FINANCIAL MANAGEMENT CONTROLS AND SYSTEMS

The Chief Financial Officers Act of 1990, the Government Performance and Results Act of 1993, the Government Management Reform Act of 1994, and the Federal Financial Management Improvement Act of 1996 were designed to improve financial management and accountability in the federal government. These statutes require the preparation of information needed by Congress, agency executives, and the public to assess management's performance and stewardship. Information required includes audit reports of agency financial statements that present an entity's financial position and results of operations. These reports must state whether an agency's financial management systems comply with federal requirements.

The Department received an unqualified (clean) opinion on its FY 2001 consolidated financial statements—the third consecutive year for this accomplishment despite continuing obstacles, including the absence of a single, integrated financial management system. (See March 2002 issue, page 83). The audits of the Department's FY 2001 statements identified two reportable conditions (one of which is considered a material weakness[1]) and several instances of noncompliance with laws and regulations, none of which was a new matter. This number of deficiencies is lower than in previous years as a result of the Department's significant progress in recognizing and recording appropriations, along with improvement in its account balance reconciliations.

Notwithstanding substantial improvements in financial management, maintaining a clean audit opinion remains a major challenge, especially under the accelerated financial reporting dates mandated by the Office of Management and Budget (OMB) for FY 2002 and beyond. Further improvements in financial management systems and operations are essential to enable the Department and its entities to correct the material weaknesses and other deficiencies identified in the audits of FY 2001 statements and produce timely, useful financial information. We

[1] Material weaknesses are serious flaws in the design or operation of an internal control component that increase the risk that errors, fraud, or noncompliance in material amounts may occur and not be readily detected.

retained an independent certified public accounting firm to audit the Department's consolidated financial statements for FY 2002 and will present the findings of this audit in our March 2003 *Semiannual Report to Congress.*

The Department recognizes the need for ongoing efforts to create a financial management environment that provides reliable financial and performance information and complies with federal laws and regulations. Such information is vital to sound decision making. Therefore Commerce continues to focus on strengthening financial management systems by implementing the Department-wide Commerce Administrative Management System to comply with federal laws and regulations and provide Commerce with accurate, timely, and reliable financial management and performance information.

The Department expects that by October 2003, Commerce's outdated and fragmented financial systems will have been replaced by CAMS. While most operating units will use CAMS, three units—International Trade Administration (ITA), U.S. Patent and Trademark Office, and National Technical Information Service—will not, but will submit data along with all other units into a Commerce-wide financial database, which will serve as the source for the Department's consolidated financial reports. The Department expects that CAMS, in conjunction with the database, will bring Commerce into compliance with federal financial systems requirements, including that for a single, integrated financial management system.

Since 1995 the Office of Inspector General has conducted reviews of the CAMS program, assessed the operational system in its annual financial statements audits, and monitored program or system progress. In recent semiannual reports we expressed concern about the management of CAMS development and maintenance, as well as the efficiency and economy of CAMS's implementation. In the last semiannual we noted that, as a result of our reviews of CAMS over the past several years, the Department has taken steps to address many of our recommendations. During this reporting period, we completed our review of program management controls at the CAMS Support Center (CSC) (see page 52). We identified a need for the Department and the center to (1) improve plans for major systems activities to support CSC's budget submission and capital asset planning, (2) track the actual cost of major system activities, (3) improve the *CAMS Capital Asset Plan* and *CAMS Quarterly Reports*, and (4) use an automated management system to monitor cost, schedule, and technical performance.

The Department's response indicates it is taking actions consistent with our recommendations: it is working to improve the CAMS budgeting process as the project moves into the operations and maintenance phase, has begun tracking actual costs as of this fiscal year, intends to improve the quarterly reports, and is working toward a performance-based management system. We will continue to monitor development and implementation of the Department's financial systems, and will keep Congress and other stakeholders informed of our findings.

CHALLENGE 2: STRENGTHEN DEPARTMENT-WIDE INFORMATION SECURITY

Commerce's information technology systems and the data they process and store are among the most critical assets of virtually all the Department's line offices and operating units. For example, NOAA's satellite, radar, and other weather forecasting data and systems protect lives and property; BIS's export license data helps control the release of dual-use commodities to foreign lands; ESA's economic indicators have policy-making and commercial value and can affect the movement of commodity and financial markets; USPTO's patent and trademark information is essential to administering patent and trademark law, promoting industrial and technical progress, and strengthening the national economy.

Keeping IT systems and data secure is of overriding importance to the Department and the entire nation: loss of or serious damage to any one of Commerce's critical systems could have devastating impacts. However, weaknesses in information security continue to exist throughout Commerce. Thus, identifying those weaknesses and recommending solutions remain a top priority for the Office of Inspector General.

During this semiannual period, OIG completed its second year of information security evaluations under the Government Information Security Reform Act (GISRA), which requires each federal agency to review its information security program annually and each OIG to perform an annual independent evaluation of that program. Agency heads must provide both of these assessments to OMB.

Our evaluation this year found that Department-level executive support for information security continues and has prompted senior management officials in the operating units to increase their attention to this area. As a result the Department has made significant progress over the past year in establishing the foundation for an effective information security program, but much remains to be done, given the severity of Commerce's information security weaknesses and the magnitude and complexity of the effort needed to address them.

For example, we found numerous systems operating without required risk assessments or approved security plans. Some that had approved security plans provided no evidence that risk analysis—a prerequisite for the security plan—had been conducted. Most operational systems have not been accredited (that is, they have not received management's formal authorization to

operate, including its explicit acceptance of risk). Those that are accredited frequently lack evidence of the requisite security testing and evaluation, thus diminishing the assurance that accreditation is intended to impart. We believe that in the coming year, the Department should focus on implementing approved security plans of adequate content and quality for all operational systems and putting those systems through rigorous certification and accreditation processes. The Department reported information security as a material weakness in its FY 2001 *Accountability Report*; we believe it should continue to be reported as such until Commerce systems that are part of the nation's critical infrastructure, as well as those that are mission critical, have been accredited (see page 53).

NIST Evaluation

As part of our Department-wide GISRA review, OIG assessed the information security program at NIST and found that the bureau is taking steps to improve its program but has yet to meet many important security requirements. At the time of our evaluation, NIST lacked a comprehensive information security program policy, did not have a documented risk assessment or approved security plan for any of its operational systems, and had accreditations for only two systems. Since the completion of our fieldwork, the director of NIST has taken important steps toward improving information security, including issuing several memorandums acknowledging responsibility for the security of NIST's data and IT systems and directing all members of senior management to give information security high priority. NIST agreed with the findings in our report and has begun to implement our recommendations (see page 39).

Separate GISRA Review for USPTO

In its efforts to position itself as a performance-based organization—given the greater independence and flexibility provided by the American Inventors Protection Act of 1999 (P.L. 106-113)—the United States Patent and Trademark Office conducts its own information security review and submits its GISRA report separately from the Department. OIG must therefore conduct a separate GISRA assessment of USPTO.

Our independent evaluation found that the Under Secretary of Commerce for Intellectual Property and Director of USPTO has made a commitment to protecting the bureau's information assets and is devoting additional attention and resources to their security. But because of inadequate attention to these matters in the past, significant weaknesses exist in USPTO's planning and budgeting for information security and implementation, review, and oversight of security measures. At the time of our evaluation, more than 80 percent of the bureau's operational systems lacked risk assessments, about one-third had outdated security plans, and none were accredited. As with Commerce as a whole, we believe that information security at USPTO is a material weakness and should be reported as such until all the bureau's mission-critical systems are accredited (see page 45).

As part of our GISRA review, we assessed USPTO's implementation of system-specific security controls, particularly focusing on the Patent Application Capture and Review System (PACR). The bureau relies on PACR to capture, store, maintain, retrieve, and print digital images of U.S. patent applications and has identified it as a highly sensitive system. We concluded that physical security measures in place during our assessment generally provide appropriate protection for PACR equipment. However, we determined that a risk assessment has not been conducted, the security plan is not approved, security controls have not been tested and reviewed, and contingency planning and specialized security training is needed. USPTO agreed with our recommendations and reported on corrective actions under way or planned (see page 46).

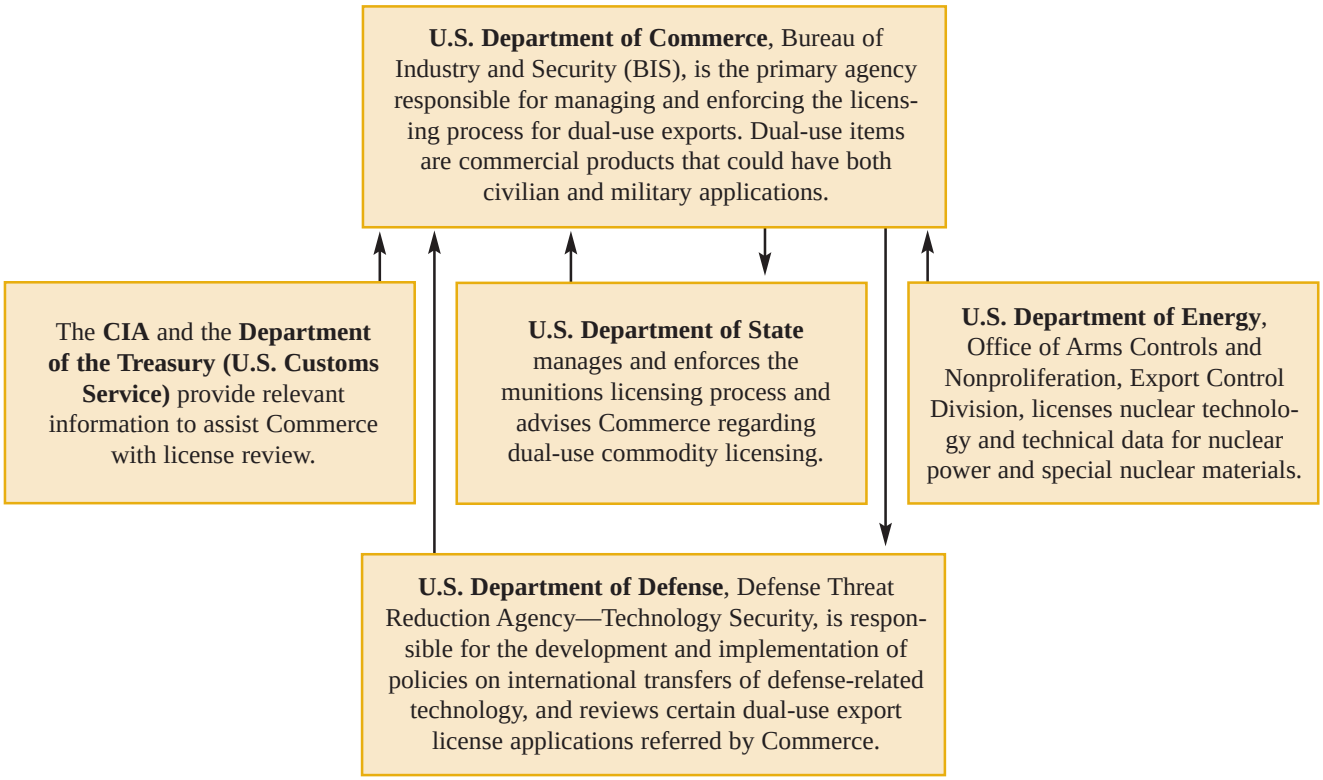
Contract Security Weaknesses

During this semiannual period we also concluded a review of the Department's IT service contracts, finding that security provisions to safeguard sensitive but unclassified systems and information were either insufficient or nonexistent. We recommended that the Department (including USPTO) establish standard contract provisions for safeguarding the security of unclassified systems and disseminate a clear, detailed policy for acquiring these systems and services. We further recommended that the Department determine whether current contracts need to be modified to include information security provisions, recognizing that in some cases contract costs could increase as a result of such changes. The Department agreed with our recommendations and is taking steps to correct the deficiencies (see page 51). We will monitor and report on its progress.

CHALLENGE 3: ENHANCE EXPORT CONTROLS FOR DUAL-USE COMMODITIES

The adequacy of export controls is a continuing concern. Opinions vary on how well the government's export control policies and practices balance the need to protect U.S. national security and foreign policy interests with the desire to promote U.S. trade opportunities and competitiveness. Striking this balance is a significant challenge for the parties involved, particularly for Commerce's Bureau of Industry and Security (BIS), which oversees the federal government's export licensing and enforcement system for dual-use commodities (goods and technologies that have both civilian and military uses).

Federal Agencies Participating in the Dual-Use Licensing Program



Strengthening dual-use export licensing and enforcement requires new, comprehensive legislative authority to replace the expired Export Administration Act of 1979 and appropriately address current export control needs and realities. Passed during the Cold War, the act sought to prevent the export of critical goods and technologies to Communist bloc countries. In today's political climate, rogue countries and terrorist groups seeking weapons of mass destruction and the systems to deliver them pose new threats to U.S. national security and foreign policy goals. Legislation is needed to address these threats, as well as to bolster BIS's regulatory authority, stiffen penalties for violations, and demonstrate America's commitment to maintaining strong export controls while encouraging other countries to do the same.

Given the importance of export controls to national security, we have devoted considerable attention to the challenges facing BIS. Specifically, we responded to a request from the Senate Governmental Affairs Committee to follow up on a 1993 interagency OIG review of the export licensing process. At the conclusion of that follow-up work, we, along with OIGs from the Central Intelligence Agency and the Departments of Defense, Energy, State, and the Treasury, issued a special interagency report in June 1999 on the export licensing processes for dual-use commodities and munitions.

Subsequently, the National Defense Authorization Act for Fiscal Year 2000, as amended, directed the inspectors general of the Departments of Commerce, Defense, Energy, State, and the Treasury, in consultation with the directors of the CIA and FBI, to report to Congress by March 31, 2000, and annually until the year 2007, on the adequacy of export controls and counterintelligence measures to prevent the acquisition of sensitive U.S. technology and technical information by countries and entities of concern. In addition, the NDAA for FY 2001 requires the OIGs to discuss in their annual interagency report the status or disposition of recommendations made in earlier reports submitted in accordance with the act. To date, we have completed three additional reviews of export controls in compliance with the act, as well as three separate follow-up reports.

Although our assessments have identified significant improvements in export controls since 1993, the 1999 report detailed some weaknesses in the licensing process. First, the processes for commodity classification and commodity jurisdiction were not timely and did not clearly specify the role of each agency. Second, the intelligence community did not review all dual-use export license applications or consistently conduct a comprehensive analysis of applications it did review, and license applications were not screened against a key database maintained

by the U.S. Customs Service. Third, there were some recurring problems with BIS's monitoring of licenses that had reporting requirements.

Subsequent OIG reviews have added items to the list of areas that require BIS's attention: the bureau needs to clarify the licensing policy and regulations regarding the release of controlled technology—commonly referred to as "deemed exports"—to foreign nationals. It also needs to conduct more outreach to federal and private research facilities to ensure that they are aware of deemed export regulations and apply for required licenses when appropriate.

The bureau also needs to improve its management of the list of controlled dual-use commodities and technologies, known as the Commerce Control List. We have recommended that BIS make the list more user-friendly, improve the timeliness with which it implements agreed-upon multilateral changes to the list, and address the inappropriate use of national security controls on some items.

Furthermore, we have several concerns about the overall effectiveness of the Committee on Foreign Investment in the United States (CFIUS), specifically CFIUS's lack of mandatory foreign investment reporting, the low number of investigations conducted on company filings, the role of the Treasury in overseeing CFIUS activities, and—within Commerce—the division of responsibilities between BIS and ITA for the CFIUS program.

The interagency OIG review team has agreed to conduct an in-depth examination of the Committee's effectiveness as part of its future work under the National Defense Authorization Act.

Upgrades to Automated Systems

During the last reporting period, we completed a review of BIS's efforts to modernize its automated licensing and enforcement systems. These enhancements are important for the Department because BIS needs a more efficient system for processing export license applications and monitoring/enforcing compliance. Our review found that BIS has made some progress on its systems redesign effort. For example, two components of the system are expected to be implemented in fiscal year 2003. However, our review also determined that BIS needed to (1) better plan to ensure the long-term success of the project and (2) implement established best practices for information technology management.

In addition to our assessment of Commerce's system, the interagency OIG review team looked at the various automated dual-use and munitions export licensing systems—maintained by Commerce, Defense, Energy, and State—to determine whether the systems could better interact and whether system modernization initiatives were in accordance with federal policies and regulations. The OIGs found limited effort to coordinate either systems interaction or systems modernization.

In the months since we issued our report on BIS, the bureau has taken action to correct some of the weaknesses we identified. However, OIG recommendations made to the relevant agency heads to help ensure better integration of the licensing systems and avoid duplication may require action by Congress or OMB.

Focused Priorities

The challenges for BIS, as well as for the administration and Congress, remain (1) passing a new Export Administration Act, (2) targeting federal licensing and enforcement efforts on those exports that present the greatest proliferation and national security risks, and (3) streamlining or eliminating controls that unnecessarily hamper trade. We will continue to monitor BIS efforts to improve dual-use export controls through the annual reviews required by the National Defense Authorization Act.

CHALLENGE 4: EFFECTIVELY MANAGE DEPARTMENTAL AND BUREAU ACQUISITION PROCESSES

Federal acquisition legislation in the 1990s mandated sweeping changes to the way federal agencies buy goods and services. Today acquisition reform initiatives are well under way, and the task before Commerce has shifted from successfully implementing reform initiatives to effectively managing the processes those initiatives have fostered. Accordingly, we have revised this top 10 challenge to reflect this new focus.

Effective acquisition processes are critical to the Department: Commerce annually spends more than $1 billion through contracts and other procurement vehicles. The Department must balance the desire to streamline the acquisition process with the need to ensure that taxpayer dollars are wisely spent and laws and regulations followed.

Acquisition reform was intended to reduce the time and money spent purchasing needed goods and services and improve the efficiency of the process. To accomplish these goals, reform initiatives encouraged contracting officers to (1) rely on performance-based service contracting and use performance-based measurement tools such as earned value and risk management, (2) consider past performance as a criterion for selecting contractors, and (3) make increased use of commercially available products. The initiatives emphasized results-based acquisition

and promoted life-cycle management of information technology as a capital investment. For high-volume, low-dollar purchases, they called for using the government purchase card whenever possible to eliminate lengthy procurement lead times.

The resulting streamlined processes, however, must not neglect basic acquisition principles: careful acquisition planning, prudent review of competitive bids, adept contract negotiations, well-structured contracts, and effective contract management. These are the principles we focus on in evaluating the Department's performance in meeting this top 10 challenge.

Government-wide, the new acquisition methods have brought new concerns. Oversight organizations such as the General Accounting Office (GAO) and OMB's Office of Federal Procurement Policy (OFPP), along with the IG community, report a variety of problems with agencies' implementation of some procurement practices.

- GAO and OIGs have identified problems with some agencies' use of purchase cards, primarily due to weak internal and administrative controls, improper purchases, lack of proper accountability, and inadequate training for cardholders.
- GAO and OFPP have found deficiencies—such as failure to obtain competitive quotes—in the use of government-wide agency contracts (GWACs) and other multiple award instruments.
- With the government's increased emphasis on competitive sourcing, GAO and OFPP remain concerned about the procurement practices of many agencies, criticizing in particular their lack of focus on results.

We also have concerns about service contracting within the Department. In past reports we have identified problems with the use of performance-based service contracting: specifically, failure to use performance-based task orders where they would be beneficial; insufficient planning for contract administration and monitoring; and the need for increased training of contracting officer's technical representatives (COTRs). In this semiannual period, we completed a review of IT service contracts throughout the Department to determine whether they contain information security provisions that adequately safeguard sensitive but unclassified systems and information. (See page 51.) We found that such provisions were either missing or inadequate and recommended that the Department develop policy, incorporate appropriate contract provisions, and require training to help ensure that contracts provide for adequate information security and that acquisition, program, and technical personnel know how to plan, implement, and manage such contracts. The Department concurred with our recommendations and is taking actions to address them.

The complex nature of certain acquisitions, such as those for performance-based IT services, increases the importance of including the whole acquisition team in the entire contracting cycle—from planning to closeout. Teams should include not only experienced contracting and procurement staff, but also program, technical, security, budget, financial, logistics, and legal personnel. We believe that the inadequacy of security provisions in IT service contracts is attributable, in part, to the lack of sufficient involvement of program managers and IT personnel during acquisition planning, requirements definition, and contract award.

Commerce has continued to implement various reform initiatives and has taken steps to improve acquisition management. Automation of the procurement process has been a primary focus, as has been the qualifications and training of the acquisition workforce. The Department's Office of Acquisition Management (OAM) has focused its attention on strengthening overall management of the procurement function within the Department and the need for additional tools and training for procurement staff. According to the Department, efforts OAM is making to improvement management include evaluating Commerce's delegation and warrant program with the goal of realigning contracting authorities to increase overall effectiveness and accountability throughout the Department's procurement community. OAM has reportedly also launched an initiative to restructure the Department-wide certification program for COTRs. This initiative includes a new training plan to enhance COTR performance and the addition of a performance plan element to improve their accountability.

OAM has taken steps to provide oversight and performance measurement of acquisition activities, using a risk management program to monitor the effectiveness of reform initiatives Department-wide. Furthermore OAM completed a review of procedures used by operating units to issue task and delivery orders under General Services Administration (GSA) Federal Supply Schedules and other multiple award contracts and is working on reviews of interagency agreements, memorandums of understanding, and purchase card policy. Finally, OAM is collaborating with the Office of the Chief Information Officer and the Commerce budget office to integrate budget and planning for IT acquisitions. We are currently reviewing purchase card activities. We will discuss our results in the next semiannual report. We will also continue to assess the status of the Department's other acquisition efforts to ensure they meet the goals of acquisition reform. Where necessary we will make recommendations for improvement.

CHALLENGE 5: ENHANCE EMERGENCY PREPAREDNESS, SAFETY, AND SECURITY OF COMMERCE FACILITIES AND PERSONNEL

As the threat of terrorism against U.S. interests has escalated at home and abroad, the need to strengthen security and emergency preparedness in both the public and private sectors has taken on new urgency. Federal agencies have rededicated themselves to ensuring the integrity of their operations, the protection of their people, their ability to continue essential services and operations during a crisis, and the suitability of risk and sensitivity designations[2] for personnel in positions of public trust. As part of this national effort, the Department has identified and addressed many of the vulnerabilities in its emergency preparedness plans and procedures and in the physical security of its facilities. It is also working to address identified vulnerabilities in its procedures for designating positions according to risk and sensitivity and for conducting appropriate background investigations of the people hired to fill sensitive and security positions. Strengthening policies and procedures to ensure the thoroughness of personnel background checks is an important step that must be taken as departmental managers strive to improve their response capabilities in emergencies and during security threats.

Homeland Security Presidential Directive-3 (HSPD-3), dated March 12, 2002, established a Homeland Security Advisory System for the nation and requires executive branch agencies to implement protective physical security measures to reduce vulnerability or increase response capability during periods of heightened alert. Subsequently the Department issued a memorandum to all Commerce operating units directing senior officials to survey their current safety status and implement any measures required by the directive that are not already in place, along with supplementary measures that local conditions may require.

In addition, Presidential Decision Directive 67, dated October 1998, directs federal agencies to develop continuity of operations plans (COOPs) to ensure the performance of essential functions during any situation that may disrupt normal operations. The chaos of September 11 highlighted the need for each federal agency to have a COOP in place that details the orderly transition to emergency operations and ensures that essential services and functions continue during a crisis, be it generated by terrorist-related incidents, natural disasters, or other events.

[2] Risk designations reflect the potential damage an individual in a position of public trust could cause to the efficiency and integrity of government programs and operations. Sensitivity designations reflect the potential adverse impact on national security associated with a position.

Complying with these directives, and related ones, is a complex, resource-intensive undertaking for Commerce, given the size of its workforce, its diverse and important missions, and the geographical spread of its approximately 500 facilities across the 50 states and 160 offices overseas. Heightened security requires a variety of measures: infrastructure risk assessments, emergency backup sites, upgraded physical security, and employee awareness and training, to name a few. The Department's personnel are being asked to safeguard life and property under emergency circumstances and to ensure that essential functions continue during any of a broad spectrum of emergencies. We believe that Commerce is making progress on many of these fronts, but the challenge is massive.

In our March 2002 report on the status of emergency preparedness and security programs at a cross-section of Commerce facilities in the Washington, D.C., area and across the nation, we concluded that significant improvements had been made since September 11 in the Department's readiness to deal with future emergencies. However, we noted that significant vulnerabilities still existed. We also identified some significant safety issues at the Commerce headquarters building in Washington, D.C., and in certain NOAA facilities in Seattle, Washington. (See March 2002 *Semiannual Report to Congress*, pages 77-82.)

Commerce's challenge to strengthen emergency preparedness, security, and safety extends to its overseas operations, especially those not collocated with U.S. embassies and consulates. In these latter situations the Department has primary responsibility for the safety and security of its people and facilities. In recent inspections of overseas posts operated by the U.S. and Foreign Commercial Service (US&FCS), we identified the need for more timely security upgrades, better management of resources, and improved oversight of security operations. (See March 2002 issue, page 40, and September 2000 issue, page 47.)

Given the heightened awareness of our vulnerability to acts of terrorism, the Department will have to regularly revisit its procedures for ensuring the safety and security of its employees and operations, and modify them as needed. We will continue to monitor its efforts in this regard and report our findings accordingly.

CHALLENGE 6: SUCCESSFULLY OPERATE U.S. PATENT AND TRADEMARK OFFICE AS A PERFORMANCE-BASED ORGANIZATION

The American Inventors Protection Act of 1999 established the U.S. Patent and Trademark Office as a performance-based organ-

ization, giving it greater flexibility and independence to operate more like a business. As such, USPTO has not only broader responsibility for managing its operations but also expanded control over its budget allocations and expenditures, personnel decisions and processes, and procurement operations.

Despite the act's potential benefits, USPTO's continuing transformation remains a formidable challenge as the agency strives to keep pace with increasingly complex technology and customer demands for higher quality products and services. In June 2002 the bureau responded to the concerns of its many stakeholders by issuing the *21st Century Strategic Plan*, which it believes will help guide the way to meeting the many challenges that have accompanied its transition to performance-based operations. The bureau must continue to develop the necessary personnel, procurement, and administrative policies, as well as performance-oriented processes and standards for evaluating cost-effectiveness, while meeting its performance goals under the Government Performance and Results Act (GPRA) and the timeliness standards of the American Inventors Protection Act.

The 5-year strategic plan, according to USPTO, is aggressive and far-reaching, and provides a road map for major changes in patent and trademark processes. It is intended to (1) reduce patent pendency from the current 25 months to 18 months by 2008, (2) move to a paperless environment and promote e-government, (3) enhance employee development, (4) explore competitive sourcing, and (5) improve and maintain quality control. USPTO's strategic plan also calls for the agency to work with worldwide intellectual property offices to create a global framework for enforcing intellectual property rights.

Agency management believes that failure to implement the new plan will delay USPTO's full implementation of e-government initiatives and increase pendency rates. It should be noted, however, that several of the initiatives envisioned in the plan-outsourcing preexamination reviews and changing fee structures, for example-require congressional approval.

During the next 2 years, we will review some of the operational changes the plan proposes. We view completion of this transition as critical to USPTO's operating success and its ability to address other challenges we identified in recent years, as described below.

Staffing to Handle Changes in Patent and Trademark Application Activity

The number of patent application filings skyrocketed in recent years. In FY 2001 USPTO received more than 326,081 applications for patents—an 8.9 percent increase over the number received in FY 2000. To address the expanding workload, USPTO hired 789 patent examiners, but lost 700 through attrition during fiscal years 2000 and 2001, virtually negating its efforts to increase staffing. Trademark filings, on the other hand, peaked in 2000 at 375,000 applications, but declined by 21 percent (to 296,000) in FY 2001. Because this downward trend is expected to continue, the bureau has started to downsize its trademark staff.

Our prior audits of USPTO reported on some of the challenges facing the bureau in recruiting and training examiners and in hiring additional administrative judges to hear appeals. As a performance-based organization, USPTO has greater flexibility to design incentives to attract and retain these highly skilled employees. During the last semiannual period we completed a review of attrition problems in two patent examiner work groups (see March 2002 issue, page 71). We made a number of recommendations for improving the screening and hiring process and thereby ultimately improving retention.

Construction of New Facility

USPTO and GSA are currently undertaking one of the federal government's largest real estate ventures—construction of USPTO's 2.4 million-square-foot office complex in Alexandria, Virginia. When completed in 2005, the 5-building complex will provide space for USPTO employees and operations currently scattered among 18 buildings in nearby Crystal City, Virginia. Now that construction has begun, USPTO must aggressively hold the line on project costs, monitor construction progress, and help ensure the project stays on schedule and within the legislatively mandated cap on the cost of completing the build-out of the facility's shell. We will be monitoring this major challenge and will follow up on issues we identified during the project's planning and design, such as space planning and allocation, relocation strategies, and actual versus target costs and completion schedules.

During construction its working title is "Building E," but USPTO will officially name this structure the Remsen Building. It is scheduled to be completed by the end of 2003.

IT Capabilities

USPTO continues to face significant challenges in delivering essential information technology capabilities. The American Inventors Protection Act of 1999 requires greater operational efficiency from the bureau, further intensifying the demands placed on IT solutions and USPTO's ability to develop new and upgrade existing systems. Our March 2002 evaluation of USPTO's information security program found that in general, the bureau's documented policies and procedures are consistent with accepted security practices, but many important security requirements are not implemented, and fundamental responsibilities are frequently not carried out (see March 2002 issue, page 74). USPTO concurred with our findings and has begun implementing our recommendations. While the results of our evaluation suggest that information security has yet to become an integral part of USPTO's business operations, the bureau's response to our recommendations indicates genuine concern about the security of its IT systems and a commitment to a stronger security program (see page 45).

CHALLENGE 7: INCREASE INTERNATIONAL COMPLIANCE WITH TRADE AGREEMENTS AND EXPAND MARKET ACCESS FOR AMERICAN EXPORTERS

To compete effectively in today's global marketplace, U.S. companies need help addressing unfair trade practices, violations of trade agreements, inadequate intellectual property protection, and other impediments to the import and export of goods and services as well as addressing confrontational situations with foreign firms operating in U.S. markets. Commerce must ensure that its trade compliance and market access efforts adequately serve U.S. companies by helping expand trade, open world markets, and eliminate unfair competition from imports priced at less than fair market value or subsidized by foreign governments.

Commerce, through various offices within the International Trade Administration, works with the Office of the U.S. Trade Representative, the Departments of State and Agriculture, and numerous other federal agencies to monitor and enforce trade agreements. The number and complexity of agreements have increased substantially in recent years.

To help in its compliance efforts, ITA created the Trade Compliance Center in 1996. The center monitors U.S. trade agreements and reviews complaints from a variety of sources. When warranted, it forms a compliance team to bring a case to satisfactory conclusion. Team members are drawn from center staff and other ITA operating units including Market Access and Compliance, Trade Development, the U.S. and Foreign Commercial Service, and other Commerce agencies, as appropriate. In addition to the activities coordinated by the center, ITA's other operating units perform a substantial amount of market access and trade compliance work. Overall, ITA's approach to trade compliance and market access is to try to solve problems at the lowest level possible—avoiding formal dispute settlement structures such as the World Trade Organization, which can take years to resolve trade disagreements.

On the import side, unfair foreign pricing and government subsidies can disrupt the free flow of goods and adversely affect U.S. companies' global competitiveness. ITA's Import Administration (IA) works with the International Trade Commission to enforce the nation's antidumping and countervailing duty laws. IA investigates complaints from U.S. industries against foreign producers and governments to determine whether dumping or subsidization has occurred and, if so, to what extent. The commission determines whether U.S. industry has suffered material injury as a result of the dumped or subsidized products. If both agencies determine that injury has occurred, IA instructs the U.S. Customs Service to assess duties against imports of those products.

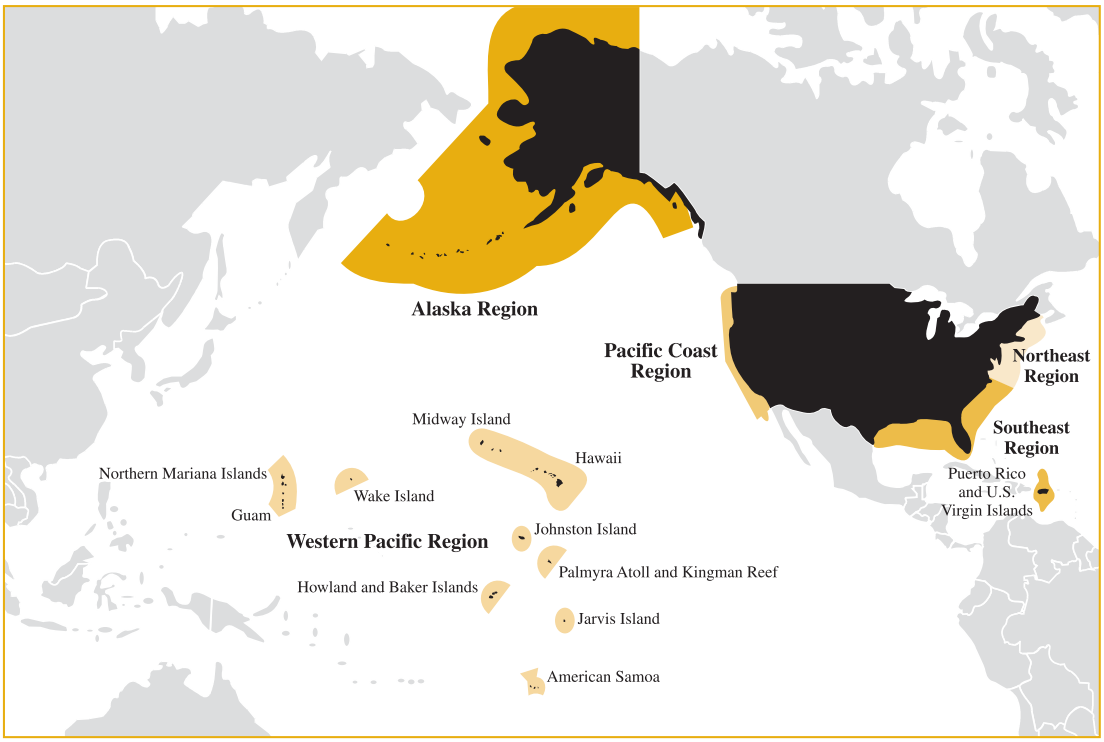
In 2001 GAO identified monitoring and enforcement of trade agreements as a major management issue for Commerce, citing two main reasons for this problem—first, the Department's shortage of staff with the expertise to monitor compliance with trade agreements, and second, its difficulty obtaining balanced, comprehensive input from the private sector.

The Secretary of Commerce has taken steps to address the concerns of both Congress and GAO by making monitoring and enforcing trade agreements a top priority for ITA and for the Department as a whole. Commerce received additional funding for trade compliance activities in FY 2001.

To effectively monitor and enforce trade agreements, ITA must maintain sufficient staff. Currently, we are reviewing ITA's ability to recruit, hire, and retain personnel for selected positions on the Market Access and Compliance staff.

To improve compliance with trade agreements, ITA also needs to promote a more coordinated federal effort. We noted that the bureau's trade agreement compliance process, as managed by the Trade Compliance Center, needs to better coordinate and track trade compliance and market access activities within ITA. The results of this review are described on page 50 of our March 2002 *Semiannual Report to Congress*.

In the future, we intend to review other aspects of ITA's approach to market access and trade compliance, as well as its administra-



The Magnuson-Stevens Act of 1976 established a U.S. exclusive economic zone (EEZ), which ranges between 3 and 200 miles offshore and consists of areas adjoining the territorial sea of the United States, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and U.S. overseas territories and possessions. NMFS is responsible for conserving and managing the fish, sea turtles, whales, seals, dolphins, and other marine mammals and their habitats within the EEZ.

tion of the antidumping and countervailing duty regulations. In the meantime, ITA must work closely with U.S. companies, other federal agencies, and foreign governments to identify trade compliance problems, develop workable solutions for them, and thus enhance American firms' access to foreign markets.

CHALLENGE 8: INCREASE THE EFFECTIVENESS OF MARINE RESOURCE MANAGEMENT

For nearly 30 years the National Marine Fisheries Service (NMFS) has had to balance two competing interests: promoting commercial and recreational fishing as vital elements of our national economy and preserving populations of fish and other marine life. The Marine Mammal Protection Act of 1972 and the Endangered Species Act of 1973 gave NMFS responsibility for preventing the extinction of marine fish, mammals, and turtles, as well as anadromous fish, such as Pacific salmon, which migrate between the ocean and inland waterways. The Magnuson-Stevens Act of 1976 made NMFS the primary federal agency for managing marine fisheries and established a regional fishery management system to help the agency carry out its mission. A 1996 amendment to the act strengthened NMFS's role in protecting and sustaining fisheries.

The Department has reported that overfishing and overcapitalization in commercial and recreational fisheries have resulted in estimated losses of billions of dollars in economic growth, thousands of jobs, and countless fishing opportunities. While certain fisheries appear to be well managed and produce positive benefits, others are severely depleted and must be restored and properly managed to realize their long-term potential. At the same time, threatened or endangered fish species need to be replenished. Among 52 distinct groups of Pacific salmon, for example, 26 are threatened or endangered.

NMFS has recently taken steps to restore Pacific salmon runs. In accordance with the Endangered Species Act, the agency's specific responsibility is to manage protected species through conservation programs and recovery plans. Its Federal Columbia River Power System 2000 Biological Opinion and the broader Federal Caucus Basin-wide Salmon Recovery Strategy established performance standards to guide recovery of Pacific salmon

in the Columbia River Basin. NMFS has also put together teams to develop recovery plans for threatened and endangered Pacific salmon species.

OIG recently evaluated the role of NMFS's Northwest Fisheries Science Center in supporting salmon recovery efforts. We focused on the center's implementation of its Salmon Research Plan, which establishes priorities to ensure that the most important scientific work is conducted. While the plan is an important step toward meeting the center's goal of strengthening its salmon research program, we found a number of deficiencies. As a result, we recommended that the center improve its peer review processes, implement comprehensive multiyear plans to measure progress in meeting the goals of the Salmon Research Plan from one year to the next, and develop better procedures for monitoring and evaluating ongoing research and related costs. (See page 32.)

We also completed a review of NMFS's plans to design and construct the first of possibly four acoustically quiet, state-of-the-art fisheries research vessels and found a number of management control weaknesses. For example, the National Oceanic and Atmospheric Administration (NOAA) has not enforced the contract's scheduling requirements, adequately tracked program costs, fully documented the program's management structure, or maintained an official contract file for the acquisition. (Details regarding these and our other findings appear on page 31.)

We are currently evaluating methods used to enforce fisheries management plans. We intend to monitor NOAA's efforts to increase the effectiveness of its marine resource management and will follow up on actions it takes in response to our recommendations regarding the Northwest Fisheries Science Center and the vessel acquisition program.

CHALLENGE 9: CONTINUE TO IMPROVE THE DEPARTMENT'S STRATEGIC PLANNING AND PERFORMANCE MEASUREMENT IN ACCORDANCE WITH THE GOVERNMENT PERFORMANCE AND RESULTS ACT

Congress and agency managers require relevant performance measures and credible performance data to effectively fulfill their oversight responsibilities with respect to federal programs. The Government Performance and Results Act of 1993 was designed to ensure the availability of such data by mandating that agencies set goals for program performance and report outcomes measured against those goals. As the administration moves toward integrating budget and performance information and using performance data to make funding decisions, the credibility of reported performance results will be critical.

Since 1997 OIG has assessed Commerce's efforts to implement GPRA. To ensure the collection and reporting of accurate, appropriate, reliable, and useful data to decision makers, this office has

- provided implementation advice and assistance,
- monitored reviews by certified public accounting firms of performance data contained in the annual financial statements,
- made presentations to departmental officials on the importance of ensuring that performance-related information is reliable,
- given informal comments to the Department on various GPRA-related documents, and
- audited internal controls for selected data on bureau performance.

Although we believe the Department has made progress toward meeting the challenge of how best to plan and measure its performance, significant opportunities for improvement remain. For one, Commerce should clearly articulate the level of reliability that can be placed on the performance data it provides in its *Annual Program Performance Report* to meet GPRA and other reporting requirements.

Also, our audits of several performance measures used by departmental units (BIS, NIST, NTIA, and USPTO) indicate a widespread need for stronger internal controls to ensure accurate reporting of performance data and improved explanations and disclosures of results. For example, procedures should be established to ensure that (1) reported information is reconciled against supporting data and (2) only data from the appropriate time period is included in performance results.

These issues are again emerging in our current audit of selected performance measures at NOAA. We are concerned that—for the measures we are evaluating—NOAA may need to (1) improve internal controls, (2) restate data that was incorrectly reported in the past, (3) provide additional disclosures and explanations of performance results, and (4) assess the value of certain measures to determine whether they should be dropped, revised, or unchanged.

We will continue to evaluate performance measurement and reporting at NOAA and other bureaus and, as warranted, make recommendations to the Department and its operating units regarding the accuracy, appropriateness, reliability, and usefulness of its performance data.

CHALLENGE 10: EFFECTIVELY MANAGE MAJOR COMMERCE RENOVATION AND CONSTRUCTION PROJECTS

The Department has plans for numerous major[3] renovation and construction projects:

- NOAA has 27 projects scheduled or in process. These include modernization of the National Ocean Service's Marine and Environmental Health Research lab in South Carolina, and a National Marine Fisheries Service lab in Hawaii.
- NIST will continue its multimillion-dollar program to upgrade existing laboratories in Gaithersburg, Maryland, and Boulder, Colorado, and to complete construction of the Advanced Measurement Laboratory building, a new facility in Gaithersburg, Maryland.
- USPTO is implementing its billion-dollar plan to consolidate employees and operations in a new, five-building facility under construction in Alexandria, Virginia (see page 8).
- The Census Bureau intends to construct two buildings at its headquarters in Suitland, Maryland, to provide employees with safe, modern facilities.
- Commerce plans to modernize its headquarters building in Washington, D.C.

Major Construction and Renovation Projects (Current and Planned as of 9/30/02)

Operating Unit	Number of Projects	EstimatedCosts (in millions)
NOAA	27	$558
NIST	2	$235
USPTO	1	$1,200
Census Bureau	1	$340
Office of the Secretary	1	$360

Note: A project may include more than one building.
Source: Commerce Office of Real Estate Policy and Major Programs.

Effective renovation and construction management is a critical challenge for the Department because of the numerous inherent risks involved in planning and managing large, costly, and complex capital improvement and construction projects. Departmental leadership and OIG oversight are needed to maximize Commerce's return on its investment in these projects. Past OIG reviews of major renovation and construction ventures have demonstrated that up-front oversight—that is, close monitoring during planning and implementation—is essential. Detecting and addressing potential problems during the developmental stages rather than after a project is completed save time and money. For this reason, we plan to actively monitor the progress of some of the Department's current and planned construction projects at Census, NIST, NOAA, USPTO, and other locations as appropriate.

[3] Projects costing $2 million or more are considered major.